



Configuration de l'accès SMB à un SVM

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Configuration de l'accès SMB à un SVM 1
 - Configuration de l'accès SMB à un SVM 1
 - Créer un SVM. 1
 - Vérifier que le protocole SMB est activé sur le SVM 2
 - Ouvrir la export policy du volume root du SVM 3
 - Créer une LIF 4
 - Activez le DNS pour la résolution du nom d'hôte. 8
 - Configurez un serveur SMB dans un domaine Active Directory 9
 - Configurer un serveur SMB dans un groupe de travail 15
 - Vérifiez les versions SMB activées 20
 - Mappez le serveur SMB sur le serveur DNS 22

Configuration de l'accès SMB à un SVM

Configuration de l'accès SMB à un SVM

Si aucune SVM n'est déjà configurée pour l'accès client SMB, vous devez créer et configurer un nouveau SVM ou configurer un SVM existant. La configuration SMB implique l'ouverture d'un accès au volume root du SVM, la création d'un serveur SMB, la création d'une LIF, l'activation de la résolution de nom d'hôte, la configuration des services de noms et, si nécessaire, Activation de la sécurité Kerberos.

Créer un SVM

Si vous ne disposez pas encore d'au moins un SVM dans un cluster pour fournir un accès aux données aux clients SMB, vous devez en créer un.

Avant de commencer

- À partir de la version ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d'informations, voir [Gestion de la capacité des SVM](#).

Étapes

1. Création d'un SVM : `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipSpace ipSpace_name`
 - Utilisez le paramètre NTFS pour le `-rootvolume-security-style` option.
 - Utilisez le paramètre par défaut C.UTF-8 `-language` option.
 - Le `ipSpace` le paramètre est facultatif.

2. Vérifier la configuration et le statut du nouveau SVM : `vserver show -vserver vserver_name`

Le `Allowed Protocols` Le champ doit inclure CIFS. Vous pouvez modifier cette liste ultérieurement.

Le `Vserver Operational State` le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'IPspace `ipSpaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipSpace ipSpaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création.

```
cluster1:> vserver show -vserver vs1.example.com
                                Vserver: vs1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: ntfs
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA
```



À partir de la ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite plafond et un seuil de débit aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir [Définissez un modèle de groupe de règles adaptatives](#).

Vérifier que le protocole SMB est activé sur le SVM

Avant de pouvoir configurer et utiliser SMB sur les SVM, il faut vérifier que le protocole est activé.

Description de la tâche

Cela s'effectue généralement lors de la configuration d'un SVM, mais si vous n'avez pas activé le protocole lors de l'installation, vous pouvez l'activer plus tard à l'aide du `vserver add-protocols` commande.



Vous ne pouvez pas ajouter ou supprimer un protocole d'une LIF une fois qu'il est créé.

Vous pouvez également désactiver les protocoles sur les SVM à l'aide de `vserver remove-protocols` commande.

Étapes

1. Vérifier les protocoles actuellement activés et désactivés pour le SVM : `vserver show -vserver vserver_name -protocols`

Vous pouvez également utiliser le `vserver show-protocols` Commande permettant d'afficher les protocoles actuellement activés sur tous les SVM du cluster.

2. Si nécessaire, activer ou désactiver un protocole :

- Pour activer le protocole SMB : `vserver add-protocols -vserver vserver_name -protocols cifs`
- Pour désactiver un protocole : `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Vérifiez que les protocoles activés et désactivés ont été correctement mis à jour : `vserver show -vserver vserver_name -protocols`

Exemple

La commande suivante affiche les protocoles actuellement activés et désactivés (autorisés et interdits) sur le SVM nommé `vs1` :

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----
vs1.example.com   cifs                        nfs, fcp, iscsi, ndmp
```

La commande suivante permet d'accéder à via SMB par ajout `cifs` Pour la liste des protocoles activés sur le SVM nommé `vs1` :

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Ouvrir la export policy du volume root du SVM

L'export policy default du volume root du SVM doit inclure une règle afin de permettre à tous les clients d'y accéder via SMB. Sans cette règle, tous les clients SMB se voient refuser l'accès au SVM et à ses volumes.

Description de la tâche

Lorsqu'un nouveau SVM est créé, une export policy par défaut (appelée `default`) est créée automatiquement pour le volume root du SVM. On doit créer une ou plusieurs règles pour l'export policy par défaut avant que les clients puissent accéder aux données sur la SVM.

Vérifiez que tous les accès SMB sont ouverts dans la stratégie d'export par défaut, puis limitez l'accès aux volumes individuels en créant des règles d'export personnalisées pour les volumes individuels ou les qtrees.

Étapes

1. Si vous utilisez un SVM existant, vérifier la root volume export policy par défaut : `vserver export-policy rule show`

Le résultat de la commande doit être similaire à ce qui suit :

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Si une telle règle existe et autorise l'accès ouvert, cette tâche est terminée. Si ce n'est pas le cas, passez à l'étape suivante.

2. Créer une règle d'export pour le volume root du SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Vérifiez la création de règles à l'aide du `vserver export-policy rule show` commande.

Résultats

Tout client SMB peut désormais accéder à n'importe quel volume ou qtrees créé sur la SVM.

Créer une LIF

Une LIF est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur up état.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions

antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).
- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

Étapes

1. Créer une LIF :

```
network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto-revert {true|false}
```

ONTAP 9.5 et versions antérieures

```
`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address -subnet-name subnet_name} -firewall-policy data -auto-revert {true false}`
```

ONTAP 9.6 et ultérieur

```
`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home-node node_name -home-port port_name {-address IP_address -netmask IP_address -subnet-name subnet_name} -firewall-policy data -auto-revert {true false}`
```

- Le `-role` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6).
- Le `-data-protocol` Paramètre n'est pas requis lors de la création d'une LIF à l'aide d'une politique de service (à partir de ONTAP 9.6). Lors de l'utilisation de ONTAP 9.5 et versions antérieures, le `-data-protocol` Le paramètre doit être spécifié lors de la création de la LIF et ne peut pas être modifié par la suite sans destruction et recréez la LIF de données.
- `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

- `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir ["Configuration des politiques de pare-feu pour les LIF"](#).

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.

2. Vérifier que le LIF a été créé correctement :

```
network interface show
```

3. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier...	Utiliser...
Adresse IPv4	<code>network ping</code>
Adresse IPv6	<code>network ping6</code>

Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé `client1_sub`) :


```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données datalif1 et datalif3 sont configurées avec des adresses IPv4 et le datalif4 est configuré avec une adresse IPv6 :

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
cluster-1	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1	clus1	up/up	192.0.2.12/24	node-1	e0a
	clus2	up/up	192.0.2.13/24	node-1	e0b
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
node-2	clus1	up/up	192.0.2.14/24	node-2	e0a
	clus2	up/up	192.0.2.15/24	node-2	e0b
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com	datalif3	up/up	192.0.2.146/30	node-2	e0c
	datalif4	up/up	2001::2/64	node-2	e0c

5 entries were displayed.

La commande suivante montre comment créer une LIF de données NAS attribuée avec le default-data-files règle de service :

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Activez le DNS pour la résolution du nom d'hôte

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

Avant de commencer

Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. Le `vserver services name-service dns create` Commande émet un avertissement si vous entrez un seul nom de serveur DNS.

Description de la tâche

Le *Network Management Guide* contient des informations sur la configuration de DNS dynamique sur le SVM.

Étapes

1. Activer le DNS sur le SVM : `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



À partir de ONTAP 9.2, le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

2. Afficher les configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande. ``

La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

Le `vserver services name-service dns check` Est disponible à partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

Configurez un serveur SMB dans un domaine Active Directory

Configurer les services de temps

Avant de créer un serveur SMB dans un contrôleur Active Domain, vous devez vous assurer que l'heure du cluster et l'heure sur les contrôleurs de domaine du domaine auquel le serveur SMB appartient correspondent dans les cinq minutes.

Description de la tâche

Vous devez configurer les services NTP du cluster de manière à utiliser les mêmes serveurs NTP pour la

synchronisation horaire que le domaine Active Directory.

Depuis ONTAP 9.5, vous pouvez configurer votre serveur NTP avec une authentification symétrique.

Étapes

1. Configurer les services de temps à l'aide du `cluster time-service ntp server create` commande.
 - Pour configurer des services de temps sans authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address`
 - Pour configurer des services de temps avec une authentification symétrique, entrez la commande suivante : `cluster time-service ntp server create -server server_ip_address -key-id key_id`
`cluster time-service ntp server create -server 10.10.10.1`
`cluster time-service ntp server create -server 10.10.10.2`
2. Vérifiez que les services de temps sont correctement configurés à l'aide du `cluster time-service ntp server show` commande.



```
cluster time-service ntp server show
```

Server	Version
-----	-----
10.10.10.1	auto
10.10.10.2	auto

Commandes de gestion de l'authentification symétrique sur les serveurs NTP

Depuis ONTAP 9.5, le protocole NTP (Network Time Protocol) version 3 est pris en charge. NTPv3 inclut une authentification symétrique à l'aide de clés SHA-1 qui augmente la sécurité du réseau.

Pour cela...	Utilisez cette commande...
Configurer un serveur NTP sans authentification symétrique	<code>cluster time-service ntp server create -server server_name</code>
Configurez un serveur NTP avec une authentification symétrique	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Activer l'authentification symétrique pour un serveur NTP existant le serveur NTP existant peut être modifié pour activer l'authentification en ajoutant l'ID de clé requis	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>

Pour cela...	Utilisez cette commande...
Configurez une clé NTP partagée	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Les clés partagées sont désignées par un ID. L'ID, son type et la valeur doivent être identiques sur le nœud et le serveur NTP</p> </div>
Configurez un serveur NTP avec un ID de clé inconnu	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
Configurez un serveur dont l'ID de clé n'est pas configuré sur le serveur NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>L'ID, le type et la valeur de clé doivent être identiques à l'ID, au type et à la valeur de clé configurés sur le serveur NTP.</p> </div>
Désactiver l'authentification symétrique	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

Créez un serveur SMB dans un domaine Active Directory

Vous pouvez utiliser le `vserver cifs create` Commande pour créer un serveur SMB sur le SVM et spécifier le domaine Active Directory (AD) auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM et à un contrôleur de domaine AD du domaine auquel vous souhaitez rejoindre le serveur SMB.

Tout utilisateur autorisé à créer des comptes machine dans le domaine AD auquel vous rejoignez le serveur SMB peut créer le serveur SMB sur la SVM. Cela peut inclure des utilisateurs d'autres domaines.

À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

Description de la tâche

Lors de la création d'un serveur SMB dans un domaine d'annuaire d'activités :

- Vous devez utiliser le nom de domaine complet (FQDN) lors de la spécification du domaine.
- Le paramètre par défaut consiste à ajouter le compte de machine du serveur SMB à l'objet CN=Computer Active Directory.

- Vous pouvez choisir d'ajouter le serveur SMB à une autre unité organisationnelle (ou) en utilisant le `-ou` option.
- Vous pouvez choisir d'ajouter une liste délimitée par des virgules d'un ou de plusieurs alias NetBIOS (jusqu'à 200) pour le serveur SMB.

La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs d'origine.

Le `vserver cifs` les pages man contiennent des paramètres facultatifs supplémentaires et des exigences de dénomination.



Depuis ONTAP 9.1, vous pouvez activer SMB version 2.0 pour vous connecter à un contrôleur de domaine (DC). Cela est nécessaire si vous avez désactivé SMB 1.0 sur les contrôleurs de domaine. Depuis ONTAP 9.2, SMB 2.0 est activé par défaut.

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine. ONTAP nécessite un cryptage pour les communications du contrôleur de domaine lorsque `-encryption-required-for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3. .

"Gestion SMB" Contient plus d'informations sur les options de configuration du serveur SMB.

Étapes

1. Vérifiez que la licence SMB est installée sur votre cluster : `system license show -package cifs`

La licence SMB est incluse avec **"ONTAP One"**. Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un domaine AD : `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

Lorsque vous entrez dans un domaine, cette commande peut prendre plusieurs minutes.

La commande suivante crée le serveur SMB "mb_server01" dans le domaine "example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

La commande suivante crée le serveur SMB "smb_server02" dans le domaine "m`ydomain.com`" et authentifie l'administrateur ONTAP avec un fichier keytab:

```
cluster1::> vsserver cifs create -vsserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. Vérifiez la configuration du serveur SMB à l'aide du `vsserver cifs show` commande.

Dans cet exemple, le résultat de la commande montre qu'un serveur SMB nommé « `SMB_SERVER01` » a été créé sur la SVM `vs1.example.com` et a été rejoint au domaine « `example.com` » domain.

```
cluster1::> vsserver cifs show -vsserver vs1

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. Si vous le souhaitez, activez la communication chiffrée avec le contrôleur de domaine (ONTAP 9.8 et versions ultérieures): `vsserver cifs security modify -vsserver svm_name -encryption -required-for-dc-connection true`

Exemples

La commande suivante crée un serveur SMB nommé « `smb_server02` » sur le SVM `vs2.example.com` dans le domaine « `example.com` » domain. Le compte machine est créé dans le conteneur « `ou=eng,ou=corp,DC=exemple,DC=com` ». Un alias NetBIOS est attribué au serveur SMB.

```
cluster1::> vsserver cifs create -vsserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vsserver cifs show -vsserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

La commande suivante permet à un utilisateur d'un domaine différent, dans ce cas un administrateur d'un domaine de confiance, de créer un serveur SMB nommé «MB_server03' » sur le SVM vs3.example.com. Le `-domain` Option spécifie le nom du domaine de départ (spécifié dans la configuration DNS) dans lequel vous souhaitez créer le serveur SMB. Le `username` spécifie l'administrateur du domaine de confiance.

- Home domain : example.com
- Domaine de confiance : trust.lab.com
- Nom d'utilisateur du domaine de confiance : Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com  
Password: . . .
```

Créez des fichiers keytab pour l'authentification SMB

Depuis ONTAP 9.7, ONTAP prend en charge l'authentification des SVM avec des serveurs Active Directory (AD) utilisant des fichiers keytab. Les administrateurs AD génèrent un fichier keytab et le rendent disponible aux administrateurs ONTAP sous la forme d'un URI (Uniform Resource identifier), qui est fourni lorsque `vserver cifs` Les commandes exigent une authentification Kerberos avec le domaine AD.

Les administrateurs D'AD peuvent créer les fichiers keytab à l'aide du serveur Windows standard `ktpass` commande. La commande doit être exécutée sur le domaine principal où une authentification est requise. Le `ktpass` la commande peut être utilisée pour générer des fichiers keytab uniquement pour les utilisateurs du domaine principal ; les clés générées à l'aide d'utilisateurs du domaine approuvé ne sont pas prises en charge.

Les fichiers keytab sont générés pour des utilisateurs ONTAP admin spécifiques. Tant que le mot de passe de l'utilisateur administrateur ne change pas, les clés générées pour le type de cryptage et le domaine spécifiques ne changent pas. Par conséquent, un nouveau fichier keytab est requis chaque fois que le mot de passe de l'utilisateur admin est modifié.

Les types de cryptage suivants sont pris en charge :

- AES256-SHA1
- DES-CBC-MD5



ONTAP ne prend pas en charge le type de cryptage DES-CBC-CRC.

- RC4-HMAC

AES256 est le type de cryptage le plus élevé et doit être utilisé si activé sur le système ONTAP.

Les fichiers keytab peuvent être générés en spécifiant le mot de passe admin ou en utilisant un mot de passe généré de manière aléatoire. Toutefois, une seule option de mot de passe peut être utilisée à un moment donné, car une clé privée spécifique à l'utilisateur admin est nécessaire au serveur AD pour déchiffrer les clés à l'intérieur du fichier keytab. Toute modification de la clé privée d'un administrateur spécifique invalidera le

fichier keytab.

Configurer un serveur SMB dans un groupe de travail

Configuration d'un serveur SMB dans une présentation d'un groupe de travail

La configuration d'un serveur SMB en tant que membre d'un groupe de travail consiste à créer le serveur SMB, puis à créer des utilisateurs et des groupes locaux.

Vous pouvez configurer un serveur SMB dans un groupe de travail lorsque l'infrastructure de domaine Microsoft Active Directory n'est pas disponible.

Un serveur SMB en mode groupe de travail prend uniquement en charge l'authentification NTLM et ne prend pas en charge l'authentification Kerberos.

Créez un serveur SMB dans un groupe de travail

Vous pouvez utiliser le `vserver cifs create` Commande permettant de créer un serveur SMB sur le SVM et de spécifier le groupe de travail auquel il appartient.

Avant de commencer

Le SVM et les LIF que vous utilisez pour transmettre des données doivent avoir été configurés pour permettre le protocole SMB. Les LIFs doivent pouvoir se connecter aux serveurs DNS configurés sur le SVM.

Description de la tâche

Les serveurs SMB en mode groupe de travail ne prennent pas en charge les fonctions SMB suivantes :

- Protocole SMB3 témoin
- Partages CA SMB3
- SQL sur SMB
- Redirection de dossiers
- Profils d'itinérance
- Objet de stratégie de groupe (GPO)
- Service Snapshot de volume (VSS)

Le `vserver cifs` les pages man contiennent des paramètres de configuration facultatifs supplémentaires et des exigences de dénomination.

Étapes

1. Vérifiez que la licence SMB est installée sur votre cluster : `system license show -package cifs`

La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Une licence CIFS n'est pas requise si le serveur SMB sera utilisé uniquement pour l'authentification.

2. Créez le serveur SMB dans un groupe de travail : `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

La commande suivante crée le serveur SMB ""mb_server01"" dans le groupe de travail ""workgroup01"":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. Vérifiez la configuration du serveur SMB à l'aide du `vserver cifs show` commande.

Dans l'exemple suivant, la sortie de la commande montre qu'un serveur SMB nommé « 'MB_server01' » a été créé sur SVM vs1.example.com dans le groupe de travail « workgroup01 » :

```
cluster1::> vserver cifs show -vserver vs0

                                Vserver: vs1.example.com
                CIFS Server NetBIOS Name: SMB_SERVER01
    NetBIOS Domain/Workgroup Name: workgroup01
        Fully Qualified Domain Name: -
                Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                Workgroup Name: workgroup01
                                Authentication Style: workgroup
    CIFS Server Administrative Status: up
                CIFS Server Description:
                List of NetBIOS Aliases: -
```

Une fois que vous avez terminé

Pour un serveur CIFS au sein d'un groupe de travail, vous devez créer des utilisateurs locaux, et éventuellement des groupes locaux, sur la SVM.

Informations associées

["Gestion SMB"](#)

Créer des comptes utilisateur locaux

Vous pouvez créer un compte utilisateur local qui peut être utilisé pour autoriser l'accès aux données contenues dans la SVM sur une connexion SMB. Vous pouvez également utiliser les comptes utilisateur locaux pour l'authentification lors de la création d'une session SMB.

Description de la tâche

La fonctionnalité des utilisateurs locaux est activée par défaut lors de la création du SVM.

Lorsque vous créez un compte utilisateur local, vous devez spécifier un nom d'utilisateur et spécifier le SVM avec lequel associer le compte.

Le `vserver cifs users-and-groups local-user` les pages man contiennent des détails sur les paramètres facultatifs et les exigences de dénomination.

Étapes

1. Créez l'utilisateur local : `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Les paramètres facultatifs suivants peuvent s'avérer utiles :

- `-full-name`

Nom complet de l'utilisateur.

- `-description`

Description de l'utilisateur local.

- `-is-account-disabled {true|false}`

Indique si le compte utilisateur est activé ou désactivé. Si ce paramètre n'est pas spécifié, la valeur par défaut est d'activer le compte utilisateur.

La commande demande le mot de passe de l'utilisateur local.

2. Entrez un mot de passe pour l'utilisateur local, puis confirmez le mot de passe.
3. Vérifiez que l'utilisateur a bien été créé : `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemple

L'exemple suivant crée un utilisateur local « SMB_SERVER01\sue, avec un nom complet « Sue Chang », associé à SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                      Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator          Built-in administrator
account
vs1      SMB_SERVER01\sue                    Sue Chang
```

Créer des groupes locaux

Vous pouvez créer des groupes locaux qui peuvent être utilisés pour autoriser l'accès aux données associées à la SVM sur une connexion SMB. Vous pouvez également attribuer des privilèges qui définissent les droits d'utilisateur ou les capacités dont dispose un membre du groupe.

Description de la tâche

La fonctionnalité de groupe local est activée par défaut lors de la création du SVM.

Lorsque vous créez un groupe local, vous devez spécifier un nom pour le groupe et vous devez spécifier la SVM avec laquelle associer le groupe. Vous pouvez spécifier un nom de groupe avec ou sans le nom de domaine local, et vous pouvez éventuellement spécifier une description pour le groupe local. Vous ne pouvez pas ajouter un groupe local à un autre groupe local.

Le `vserver cifs users-and-groups local-group` les pages man contiennent des détails sur les paramètres facultatifs et les exigences de dénomination.

Étapes

1. Créez le groupe local : `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

Le paramètre facultatif suivant peut être utile :

- ° `-description`

Description du groupe local.

2. Vérifiez que le groupe a bien été créé : `vserver cifs users-and-groups local-group show -vserver vserver_name`

Exemple

L'exemple suivant crée un groupe local « ``SMB_SERVER01\engineering` » associé à la SVM `vs1`:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

Vserver	Group Name	Description
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

Une fois que vous avez terminé

Vous devez ajouter des membres au nouveau groupe.

Gérer l'appartenance à un groupe local

Vous pouvez gérer l'appartenance à un groupe local en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et supprimant des groupes de domaines. Cette option est utile si vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe.

Description de la tâche

Si vous ne souhaitez plus qu'un utilisateur local, un utilisateur de domaine ou un groupe de domaines dispose de droits d'accès ou de privilèges en fonction de l'appartenance à un groupe, vous pouvez supprimer le membre du groupe.

Lorsque vous ajoutez des membres à un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial *Everyone*.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, ONTAP doit pouvoir résoudre le nom en SID.

Lorsque vous supprimez des membres d'un groupe local, vous devez garder à l'esprit les éléments suivants :

- Vous ne pouvez pas supprimer des membres du groupe spécial *Everyone*.
- Pour supprimer un membre d'un groupe local, ONTAP doit pouvoir résoudre son nom en SID.

Étapes

1. Ajouter un membre à un groupe ou en supprimer.

- Ajouter un membre : `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à ajouter au groupe local spécifié.

- Supprimer un membre : `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à supprimer du groupe local spécifié.

Exemples

L'exemple suivant ajoute un utilisateur local « `SMB_SERVER01\sue` » au groupe local « `SMB_SERVER01\engineering` » sur le SVM `vs1.example.com` :

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

L'exemple suivant supprime les utilisateurs locaux « `SMB_SERVER01\sue` » et « `SMB_SERVER01\james` » du

groupe local « `SMB_SERVER01\engineering' » sur la SVM vs1.example.com :

```
cluster1::> vserver cifs users-and-groups local-group remove-members  
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names  
SMB_SERVER\sue,SMB_SERVER\james
```

Vérifiez les versions SMB activées

Votre version de ONTAP 9 détermine quelles versions de SMB sont activées par défaut pour les connexions avec les clients et les contrôleurs de domaine. Vérifiez que le serveur SMB prend en charge les clients et les fonctionnalités requis dans votre environnement.

Description de la tâche

Pour les connexions avec les clients et les contrôleurs de domaine, vous devez activer SMB 2.0 et versions ultérieures autant que possible. Pour des raisons de sécurité, évitez d'utiliser SMB 1.0 et désactivez-le si vous avez vérifié qu'il n'est pas nécessaire dans votre environnement.

Dans ONTAP 9, SMB version 2.0 et ultérieure est activé par défaut pour les connexions client, mais la version de SMB 1.0 activée par défaut dépend de votre version de ONTAP.

- Depuis la version ONTAP 9.1 P8, SMB 1.0 peut être désactivé sur les SVM.

Le `-smb1-enabled` à la `vserver cifs options modify` La commande active ou désactive SMB 1.0.

- Depuis ONTAP 9.3, il est désactivé par défaut sur les nouveaux SVM.

Si votre serveur SMB se trouve dans un domaine Active Directory (AD), vous pouvez activer SMB 2.0 pour vous connecter à un contrôleur de domaine (DC), à partir de ONTAP 9.1. Cela est nécessaire si vous avez désactivé SMB 1.0 sur DCS. Depuis ONTAP 9.2, SMB 2.0 est activé par défaut pour les connexions CC.



Si `-smb1-enabled-for-dc-connections` est défini sur `false` pendant `-smb1-enabled` est défini sur `true`, ONTAP refuse les connexions SMB 1.0 en tant que client, mais continue à accepter les connexions SMB 1.0 entrantes en tant que serveur.

"Gestion SMB" Le contient des détails sur les versions et fonctionnalités SMB prises en charge.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Vérifiez les versions SMB activées :

```
vserver cifs options show
```

Vous pouvez faire défiler la liste pour afficher les versions SMB activées pour les connexions client et si

vous configurez un serveur SMB dans un domaine AD, pour les connexions de domaine AD.

3. Activez ou désactivez le protocole SMB pour les connexions client si nécessaire :

- Pour activer une version SMB :

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- Pour désactiver une version SMB :

```
vserver cifs options modify -vserver vserver_name smb_version false
```

Valeurs possibles pour `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

La commande suivante active SMB 3.1 sur le SVM `vs1.example.com` :

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. Si votre serveur SMB se trouve dans un domaine Active Directory, activez ou désactivez le protocole SMB pour les connexions DC selon les besoins :

- Pour activer une version SMB :

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- Pour désactiver une version SMB :

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. Retour au niveau de privilège admin :

```
set -privilege admin
```

Mappez le serveur SMB sur le serveur DNS

Le serveur DNS de votre site doit avoir une entrée pointant sur le nom du serveur SMB, et tous les alias NetBIOS, à l'adresse IP de la LIF de données afin que les utilisateurs Windows puissent mapper un disque au nom du serveur SMB.

Avant de commencer

Vous devez avoir un accès administratif au serveur DNS de votre site. Si vous ne disposez pas d'un accès administratif, vous devez demander à l'administrateur DNS d'effectuer cette tâche.

Description de la tâche

Si vous utilisez des alias NetBIOS pour le nom du serveur SMB, il est recommandé de créer des points d'entrée de serveur DNS pour chaque alias.

Étapes

1. Connectez-vous au serveur DNS.
2. Créer des entrées de recherche de type a - Address record (enregistrement d'adresse A) et inverse (PTR - enregistrement du pointeur) pour mapper le nom du serveur SMB à l'adresse IP de la LIF de données.
3. Si vous utilisez des alias NetBIOS, créez une entrée de recherche alias nom canonique (enregistrement de ressource CNAME) pour mapper chaque alias à l'adresse IP de la LIF de données du serveur SMB.

Résultats

Une fois le mappage propagé sur le réseau, les utilisateurs Windows peuvent mapper un lecteur au nom du serveur SMB ou à ses alias NetBIOS.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.